

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
An Apple iPhone Bearing IMEI Number
354820294006550 Currently Located at DEA
Greensboro Resident Office

Case No. 1:24MJ517-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841(a)(1), 843(a)(3), and 846	Distrib. & PWID Controlled Subs., Obtain Controlled Subs. by Fraud, Conspiracy to Distib. & PWID Controlled Subs.

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Glen Sakamura

Applicant's signature

DEA TFO Glen Sakamura

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means).

Date: 12/2/2024 8:34 am

City and state: Durham, North Carolina



Judge's signature

Joe L. Webster, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE BEARING IMEI
NUMBER 354820294006550, CURRENTLY
LOCATED AT DEA GREENSBORO
RESIDENT OFFICE, 1801 STANLEY
ROAD, SUITE 201, GREENSBORO,
NORTH CAROLINA 27407

Case No. 1:24MJ517-1

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Glen Sakamura, having been duly sworn, depose and state:

INTRODUCTION

1. I am employed as a Task Force Officer with the U.S. Drug Enforcement Agency (DEA) and have been so employed since May 2023. In my capacity as a DEA Task Force Officer, I prevent, detect, and investigate offenses under Title 21 of the United States Code and Title 21 of the Code of Federal Regulations. Typical investigations involve physicians, pharmacists, and others who engage in the manipulation of records, invoices, and prescriptions to conceal criminal activities. Additionally, many of these investigations involve the use of internet websites and other electronic communications, which help to facilitate these activities.

2. I am a federal law enforcement officer of the United States within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure. My responsibilities include investigations of alleged criminal violations of prescription drug diversion, conduct complex narcotic criminal investigations, and related offenses. I have received extensive training in drug diversion and distribution schemes. As a detective with the Randolph County Sheriff's Office and as a DEA

Task Force Officer, I have been involved in hundreds of drug investigations and cases at local, state, and federal levels.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device, specifically, a cell phone (“SUBJECT DEVICE”)—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1) and 846 have been committed by Shaniyah JACKSON, and others. I further submit that based on the evidence set forth below, and all reasonable inferences from that evidence, there is probable cause to believe that evidence, instrumentalities, and/or fruits of these crimes, as further described in Attachment B, will be found on SUBJECT DEVICE, as identified in Attachment A.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is an Apple iPhone, bearing IMEI Number 354820294006550, utilizing phone number 585-413-6519, hereinafter the “the SUBJECT DEVICE.” The SUBJECT DEVICE was seized on November 27, 2024 from JACKSON incident to her arrest and is currently located at DEA at the Greensboro Resident Office, 1801 Stanley Road, Suite 201, Greensboro, North Carolina 27407. The applied-for warrant would authorize the forensic

examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. I know from my training and experience that individuals who engage in criminal activity, including drug diversion and distribution, use cell phones to: (1) access websites to facilitate illegal activity, (2) communicate with co-conspirators about the scheme, (3) to store on digital devices, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators, email correspondence, text or other “Short Message Service” (“SMS”) messages, contact information of co-conspirators, financial data, including bank account numbers and information, cryptocurrency wallets and passwords, and credit card numbers, (4) keep track of co-conspirator’s contact information, (5) keep a record of illegal transactions for future reference, and (6) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators.

8. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing photographs and videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may

also include global positioning system (“GPS”) technology for determining the location of the device.

9. In or about December 2023, agents with the DEA Greensboro Resident Office initiated an investigation and collaborated with the Columbia, SC District Office and Charlotte, NC District Office regarding a criminal investigation involving an organized drug trafficking organization that is using legitimate DEA registration numbers to create large quantities of fraudulent electronic prescriptions for controlled substances for illegitimate sale and profit. This scheme uncovered that many DEA registration numbers¹, which are required to write prescriptions for controlled substances, were pilfered and utilized to illicitly write fraudulent electronic prescriptions for Schedule II-V controlled substances for patients who do not exist. This scheme included fraudulently writing and sending large amounts of prescriptions during weekend hours to pharmacies located in four different states, including North Carolina. Sending prescriptions over the weekend minimized the chance that pharmacists would call doctors to confirm prescriptions since most doctor’s offices are closed on the weekends. These prescriptions were created in an online prescription software program and sent to various, specific pharmacies on the east coast of the United States to be filled. The drug trafficking organization would then employ individuals to go to these pharmacies to pick up and pay for the filled controlled substance prescriptions. Based on intelligence received from the DEA Columbia, SC District Office, the individuals who were

¹ A DEA registration number is a unique identifier given by the Drug Enforcement Administration to medical practitioners, such as pharmacists, nurse practitioners, doctors, and dentists, which allows them to prescribe, dispense, and administer drugs defined as controlled substances.

picking up the controlled substances from the pharmacies in North and South Carolina were from the New England area.

10. In or about February 2024, DEA Greensboro Resident Office investigations revealed that one of the DEA registrants whose number was illegitimately used was Dr. Alexis Henderson. Photocopies of the fraudulent prescriptions from the various pharmacies were obtained with Dr. Alexis Henderson's DEA registration number. A query of North Carolina's Controlled Substance Reporting System (NC CSRS) revealed approximately 18 prescriptions for Schedule II-V controlled substances were issued under Dr. Henderson's DEA registration number and filled throughout North Carolina between September 24, 2023 and September 28, 2023. The fraudulently issued electronic prescriptions were sent to various chain pharmacies such as CVS, Walgreens, and Publix, as well as independently owned retail pharmacies.

11. The North Carolina Board of Pharmacy requires individuals picking up filled Schedule II controlled substance prescriptions to provide identification to the pharmacy in order to dispense the prescription. DEA Diversion Investigators retrieved copies of the fraudulently filled electronic prescriptions, identifying information for the individual picking up the prescription, driver's license information for the individual picking up the prescription, and video footage capturing the transaction from several area pharmacies. Shaniyah JACKSON was identified through both sign out logs and her scanned Florida driver's license as one of the individuals who picked up and paid for the controlled substances dispensed from the fraudulent electronic prescriptions issued through Dr. Henderson's DEA registration number. Security footage from an area pharmacy showed JACKSON in the pharmacy purchasing the controlled substances.


12. After identifying JACKSON, DEA agents ran JACKSON's name through multiple law enforcement databases. JACKSON has been identified as member and runner within the Devin

Anthony MAGARIAN drug trafficking organization. MAGARIAN has been indicted in the United States District Court for the Eastern District of New York (EDNY) for conspiracy to distribute and possess with intent to distribute oxycodone, in violation of 21 USC 841(a) and 846, among other charges.

13. Telegram messages between MAGARIAN, utilizing telephone number 603-851-3756, and JACKSON, utilizing telephone number 585-413-6519, show that MAGARIAN's primary Florida accomplice appears to be JACKSON, who utilizes phone number 585-413-6519 and Cashapp usernames Niyahh\$3, \$mariasanch3z, \$jthom343. JACKSON is saved in MAGARIAN's phone as "Shaynia" and is referred to as Shaynia several times in conversations with others. JACKSON uses the online handle "Maria Sanchez" on Telegram and has approximately 4,242 text message exchanges between herself and MAGARIAN—the most of any of MAGARIAN's contacts. JACKSON and MAGARIAN appear to obtain and fill fraudulent prescriptions themselves for months before MAGARIAN expanded his network to other individuals and states. JACKSON and MAGARIAN appear to have a close relationship, and JACKSON provides MAGARIAN her personal login information and payment methods to book rental cars, hotels, and plane.

14. JACKSON appears to have picked up drugs provided by fraudulent prescriptions in Florida, Texas, Georgia, and North Carolina, often using rental cars to travel and obtain them.

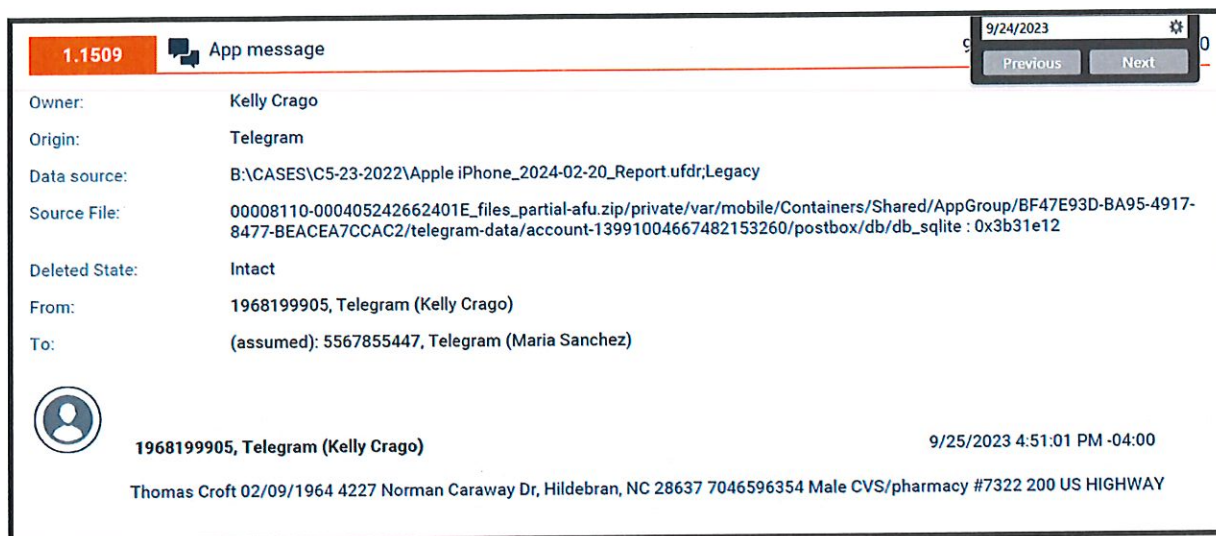
15. On September 25, 2023, MAGARIAN sent JACKSON patient, prescription, and pharmacy information located in Statesville, North Carolina:

Owner:	Kelly Crago	Previous	Next
Origin:	Telegram		
Data source:	B:\CASES\C5-23-2022\Apple iPhone_2024-02-20_Report.ufdr;Legacy		
Source File:	00008110-000405242662401E_files_partial-afu.zip/private/var/mobile/Containers/Shared/AppGroup/BF47E93D-BA95-4917-8477-BEACEA7CCAC2/telegram-data/account-13991004667482153260/postbox/db/db_sqlite : 0x3b8f889		
Deleted State:	Intact		
From:	1968199905, Telegram (Kelly Crago)		
To:	(assumed): 5567855447, Telegram (Maria Sanchez)		
		1968199905, Telegram (Kelly Crago) 9/25/2023 4:51:01 PM -04:00	
Katherine Bowlds 05/10/1963 194 Wilderness Ln, Statesville, NC 28687 7044424997 Female CVS/pharmacy #3524 215 NORTH CENTER STREET, STATESVILLE, NC 28677 (704) 872-6593 Sent oxy & ibuprofen successfully. 92/256			

16. According to prescription data, pharmacy records, and video from September 25, 2023, JACKSON picked up a prescription for 90 oxycodone 30 mg tablets at CVS Pharmacy #3524 in Statesville, NC. JACKSON presented her Florida Driver's license number J250781039180 while picking up the fraudulent prescription.

17. According to law enforcement databases, Florida Driver's License number J250781039180 is associated with Shaniyah Amarie Sanchez. Further search of law enforcement database records indicate that Shaniyah Amarie Sanchez also goes by the alias, Shaniyah JACKSON.

18. On September 25, 2023, MAGARIAN sent JACKSON the following patient, prescription, and pharmacy information located in Hildebran, North Carolina:



19. According to prescription data, pharmacy records, and video from September 25, 2023, JACKSON picked up a prescription for 90 oxycodone 30 mg tablets at CVS Pharmacy #7322 in Hildebran, NC. JACKSON presented her Florida Driver's license number J250781039180 while picking up the fraudulent prescription.

20. According to travel records, on September 24, 2023, FENDERSON traveled from Manchester-Boston Regional Airport (MHT) to Charlotte international Airport (CLT) on American Airlines on Flight 5457. According to Hertz rental car records, FENDERSON rented a vehicle bearing NC license plate number KJA3518 at approximately 2:17 PM. Toll records from September 24, 2023, indicate FENDERSON, using telephone number 603-851-2251, received a call from telephone number 505-413-6519, which is associated with JACKSON at approximately 2:31 PM. According to cell site records, FENDERSON was located at Charlotte Douglas International Airport, when the call occurred.

ARREST OF JACKSON AND SEIZURE OF DEVICE

1. On October 28, 2024, a Grand Jury in the Middle District of North Carolina returned a true bill of indictment against JACKSON and other co-conspirators, based on probable cause that JACKSON had violated 21 U.S.C. § 846.

2. On November 27, 2024, law enforcement officers arrested JACKSON in Orlando, Florida.

3. At the time of arrest, DEA agents seized JACKSON's belongings incident to arrest, including a cellular telephone that JACKSON was using minutes before the arrest. The cellular device was shipped to the DEA's Greensboro Resident Office immediately after seizure.

4. The SUBJECT DEVICE is currently in the lawful possession of the DEA. It came into the DEA's possession after being seized incident to arrest. The SUBJECT DEVICE is currently in storage at the DEA Greensboro Resident Office, 1801 Stanley Road, Suite 201, Greensboro, North Carolina 27407. In my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of the DEA.

TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives.

This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control

a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

6. Based on my training, experience I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and handheld computer. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

7. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

8. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

9. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many

parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

10. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

11. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B, and for this court to authorize execution of the warrant at any time in the day or night.

/s/ Glen Sakamura
Glen Sakamura, Task Force Officer
Drug Enforcement Administration

On this 2nd day of December 2024, Glen Sakamura appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit. 8:34 am



HON. JOEL L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of the Subject Device to be Searched

1. The SUBJECT DEVICE is an Apple iPhone, bearing IMEI354820294006550, using telephone number 585-413-6519, that is currently located at the U.S. Drug Enforcement Agency at the Greensboro Resident Office, 1801 Stanley Road, Suite 201, Greensboro, North Carolina 27407.

ATTACHMENT B

Items to be Seized

The following materials, which constitute evidence of the commission of federal offenses, contraband, the fruits of the crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 21 U.S.C. §§ 841(a)(1), 843(a), and 846 involving Shaniyah JACKSON in the form of:

1. Records, information, and communications revealing or referencing the possession or distribution of controlled substances;
2. Records, information, and communications revealing or referencing the creation or use of prescriptions;
3. Records, information, and communications revealing or referencing procurement or use of practitioners' DEA registration numbers;
4. Records, information, and communications revealing or referencing the creation or use of fake identities for the prescriptions;
5. Records, information, and communications revealing or referencing the proceeds of the crimes under investigation;
6. Records, information, and communications revealing or referencing items commonly associated with trafficking in controlled substances, such as scales, plastic baggies, money counters, and safes;
7. Records, information, and communications revealing or referencing controlled substance customers;
8. Records, information, and communications revealing or referencing the identity of co-conspirators of the crimes under investigation; and

9. Records, information, and communications revealing or referencing the location and identity of the user of the phone at the approximate times the aforementioned records and information were created, deleted, or interacted with.

For the cellphone whose search is otherwise authorized by this warrant (hereinafter COMPUTER):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.